Алексей Хлебников

OpenSSL 3: ключ к тайнам криптографии



ДМК Пресс
Издательство

Содержание

От издательства 13

Вступительное слово 14

Об авторе 15

О рецензенте 16

Предисловие 17

Часть I. Введение 21

Глава 1. OpenSSL и другие библиотеки SSL/TLS 22

Что такое OpenSSL? 22
История OpenSSL 24
Что нового в OpenSSL 3.0? 24
Сравнение OpenSSL с GnuTLS 25
Сравнение OpenSSL с NSS 26
Сравнение OpenSSL с Botan 27
Сравнение OpenSSL с облегченными библиотеками TLS 27
Сравнение OpenSSL с LibreSSL 29
Сравнение OpenSSL с BoringSSL 30
Резюме 31

Часть II. Симметричная криптография 32

Глава 2. Симметричное шифрование и расшифрование 33

Технические требования 33
Что такое симметричное шифрование 34
Обзор симметричных шифров, поддерживаемых OpenSSL 35

Сравнение блочных и потоковых шифров 35
Стойкость симметричного шифра 37
Сколько битов стойкости достаточно? 38
Обзор шифра AES 38
Обзор шифров DES и 3DES 39
Обзор шифра RC4 40
Обзор шифра ChaCha20 40
Обзор других симметричных шифров, поддерживаемых OpenSSL 41
Национальные шифры 41
Семейство шифров RC 43
Другие шифры 43
Режимы работы блочных шифров 44
Обзор режима простой замены 44
Обзор режима простой замены с зацеплением 45
Обзор режима CTR 47
Обзор режима GCM 48
Обзор режима AES-GCM-SIV 51
Другие режимы работы блочных шифров 51
Выбор режима работы блочного шифра 52
Дополнение для блочных шифров 52
Как сгенерировать ключ симметричного шифрования 53
Скачивание и установка OpenSSL 54
Шифрование и расшифрование с применением AES в командной строке 56
Инициализация и очистка библиотеки OpenSSL 60
Компиляция и компоновка с OpenSSL 61
Шифрование с применением AES из программы 63
Реализация программы шифрования 64
Выполнение программы encrypt 67
Расшифрование с применением AES из программы 68
Реализация программы decrypt 68
Выполнение программы decrypt 70
Резюме 71

Глава 3. Хеш-значения сообщений 72

Технические требования 72
Что такое хеш-значение сообщения и криптографическая функция хеширования? 73
Зачем нужны хеши сообщений? 74
Проверка целостности данных 74
Хеш-значения как основа HMAC 74
Цифровые подписи 75
Сетевые протоколы 75
Проверка пароля 75
Идентификатор содержимого 75
Блокчейн и криптовалюты 76

Доказательство выполнения работы 76
Оценка стойкости криптографических функций хеширования 77
Обзор криптографических функций хеширования, поддерживаемых OpenSSL 78
Семейство функций хеширования SHA-2 78
Семейство криптографических функций SHA-3 79
Функции хеширования SHA-1 и SHA-0 81
Семейство функций хеширования MD 82
Семейство функций хеширования BLAKE2 83
Менее популярные функции хеширования, поддерживаемые OpenSSL 84
Национальные криптографические функции хеширования 84
Другие криптографические хеш-функции 84
Какую криптографическую функцию хеширования выбрать? 85
Вычисление хеш-значения в командной строке 85
Вычисление хеш-значения из программы 86
Реализация программы digest 87
Выполнение программы digest 88
Резюме 88

Глава 4. MAC и HMAC 89

Технические требования 89
Что такое имитовставка? 90
Стойкость функции вычисления MAC 90
HMAC – MAC на основе функции хеширования 91
MAC, шифрование и принцип криптографической обреченности 93
Вычисление HMAC в командной строке 95
Вычисление HMAC из программы 96
Реализация программы hmac 97
Выполнение программы hmac 98
Резюме 98

Глава 5. Формирование ключа шифрования из пароля 100

Технические требования 100
В чем разница между паролем и ключом шифрования? 101
Что такое функция формирования ключа? 101
Обзор функций формирования ключа, поддерживаемых OpenSSL 104
Формирование ключа из пароля в командной строке 105
Формирование ключа из пароля из программы 105
Реализация программы kdf 106
Выполнение программы kdf 107
Резюме 108

Часть III. Асимметричная криптография и сертификаты 109

Глава 6. Асимметричное шифрование и расшифрование 110

Технические требования 110
Что такое асимметричное шифрование 111
Что такое атака с человеком посередине 111
Личная встреча 112
Проверка цифрового отпечатка ключа по телефону 112
Разделение ключа 113
Подписание ключа доверенной третьей стороной 113
Какие виды асимметричного шифрования доступны в OpenSSL 113
Что такое сеансовый ключ 114
Криптостойкость RSA 115
Генерирование пары ключей RSA 118
Шифрование и расшифрование с помощью RSA в командной строке 120
Шифрование с помощью RSA из программы 122
Реализация программы rsa-encrypt 123
Выполнение программы rsa-encrypt 125
Что такое очередь ошибок в OpenSSL 126
Расшифрование с помощью RSA из программы 129
Реализация программы rsa-decrypt 130
Выполнение программы rsa-decrypt 131
Резюме 131

Глава 7. Цифровые подписи и их проверка 132

Технические требования 133
Что такое цифровая подпись 133
Различие между цифровыми подписями и имитовставками 134
Обзор алгоритмов цифровых подписей, поддерживаемых OpenSSL 135
Алгоритм RSA 135
Алгоритм DSA 135
Алгоритм ECDSA 136
Алгоритм EdDSA 137
Алгоритм SM2 138
Какой алгоритм цифровой подписи выбрать? 139
Генерирование пары ключей эллиптического шифрования 139
Подписание и проверка подписи в командной строке 141
Подписание из программы 142
Реализация программы ec-sign 143
Выполнение программы ec-sign 145
Проверка подписи из программы 145
Реализация программы ec-verify 146
Выполнение программы ec-verify 147
Резюме 148

Глава 8. Сертификаты X.509 и инфраструктура открытых ключей 149

Технические требования 150
Что такое сертификат X.509? 150
Цепочки сертификатов 152
Как выпускаются сертификаты X.509 156
Что такое расширения X509v3? 159
Инфраструктура открытых ключей X.509 159
Генерирование самоподписанного сертификата 160
Генерирование несамоподписанного сертификата 162
Проверка сертификата в командной строке 165
Проверка сертификата из программы 166
  Реализация программы x509-verify 166
  Выполнение программы x509-verify 168
Резюме 169

Часть IV. TLS-подключения и безопасная связь 170

Глава 9. Установление TLS-подключений и передача по ним данных 171

Технические требования 172
Что такое протокол TLS 172
  TLS-квитирование 174
  Что происходит после TLS-квитирования? 176
История протокола TLS 177
Установление клиентского TLS-подключения в командной строке 180
Подготовка сертификатов для подключения к TLS-серверу 181
Прием запроса на подключение к TLS-серверу в командной строке 183
Базовые объекты ввода-вывода в OpenSSL 183
Установление клиентского TLS-подключения из программы 186
  Реализация программы tls-client 187
  Выполнение программы tls-client 190
Прием запроса на подключение к TLS-серверу из программы 191
  Реализация программы tls-server 192
  Выполнение программы tls-server 197
Резюме 199

Глава 10. Использование сертификатов X.509 в TLS 200

Технические требования 200
Специальная проверка сертификата другой стороны в программах на C 201
  Регистрация функции обратного вызова для проверки 203
  Реализация функции обратного вызова для проверки 204

Выполнение программы ... 207
Использование списков отозванных сертификатов в программах на C ... 208
Регистрация функции обратного вызова для поиска в CRL ... 210
Реализация функции обратного вызова для поиска в CRL ... 211
Реализация функции скачивания CRL с точки распространения ... 213
Реализация функции скачивания CRL с URL-адреса типа HTTP ... 214
Выполнение программы ... 216
Протокол онлайновой проверки состояния сертификата ... 217
Что такое протокол онлайновой проверки состояния сертификата ... 217
Использование OCSP в командной строке ... 218
Использование OCSP в программах на C ... 221
Регистрация функции обратного вызова для OCSP ... 223
Реализация функции обратного вызова для OCSP ... 223
Выполнение программы ... 227
Использование клиентских сертификатов в TLS ... 228
Генерирование клиентских сертификатов TLS ... 228
Упаковка клиентских сертификатов в контейнер PKCS #12 ... 229
Программный запрос и проверка клиентского сертификата TLS на стороне сервера ... 230
Проверка клиентского сертификата TLS ... 231
Реализация функции построения ответа ... 232
Выполнение программы ... 233
Программное установление TLS-подключения с клиентским сертификатом ... 235
Изменение кода, унаследованного от программы tls-client ... 236
Загрузка сертификата TLS-клиента ... 237
Выполнение программы ... 240
Резюме ... 240

Глава 11. Специализированные применения TLS ... 242

Технические требования ... 242
Что такое закрепление сертификатов в TLS ... 243
Использование закрепления сертификатов ... 245
Изменение функции run_tls_client() ... 246
Реализация функции cert_verify_callback() ... 248
Выполнение программы tls-cert-pinning ... 249
Что такое блокирующие и неблокирующие сокеты ... 251
Использование неблокирующих сокетов в TLS ... 252
Изменение функции run_tls_client() ... 252
Выполнение программы tls-client-non-blocking ... 257
Что такое TLS на нестандартных сокетах ... 258
Использование TLS на нестандартных сокетах ... 259
Реализация функции service_bios() ... 260
Переработанная функция run_tls_client() ... 262
Выполнение программы tls-client-memory-bio ... 267
Резюме ... 269

Часть V. Мини-УЦ 270

Глава 12. Эксплуатация мини-УЦ 271

Технические требования 271
Подкоманда openssl ca 271
Генерирование сертификата корневого УЦ 273
Генерирование сертификата промежуточного УЦ 278
Генерирование сертификата для веб-сервера 282
Генерирование сертификата веб-клиента и почтового клиента 283
Отзыв сертификатов и генерирование CRL 285
Информирование о состоянии отзыва сертификатов по протоколу OCSP 288
Резюме 291

Предметный указатель 292